<Insert Name of Engagement Here>
Security Assessment Findings Report

Your Name

Business Confidential

Date: Date here
Project: 2020-001

Version 1.0

Table of Contents

Table of Contents....3
Confidentiality Statement....3
Disclaimer....3
Contact Information....4
Assessment Overview....5
Assessment Components....5
External Penetration Test....5
Internal Penetration Test....5
Scope....6
Scope Exclusions....6
Client Allowances....6
Executive Summary....7
Testing Summary....7
Security Strengths....7
Insert a Strength Here....7
Insert a Strength Here....7
Security Weaknesses....7
Insert a Weakness Here....7
Insert a Weakness here....7
Penetration Test Findings....8
Insert the Vulnerability Here – Insert IP address or other information....8
Insert the Vulnerability Here – Insert IP address or other information....9

Confidentiality Statement

This document is the exclusive property of **<Insert Client>** and **<your name>**. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both **<Insert Client>** and **<your name>**.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. <**yourname**> prioritized the assessment to identify the weakest security controls an attacker would exploit.

<yourname> recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

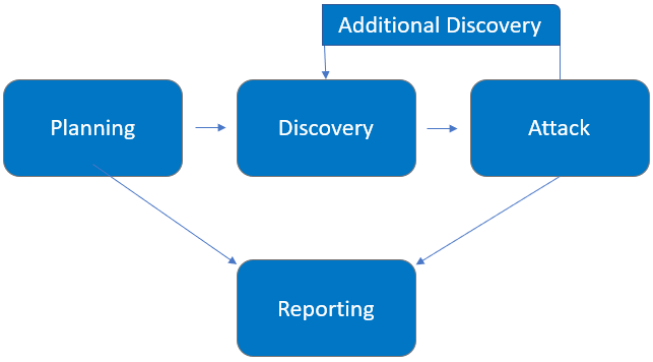
Name	Title	Contact Information
Client Name Here		
John Smith	Insert Title	Office: (555) 555-5555 Email: john.smith@demo.com
Your Org Here		
Your Name	Lead Penetration Tester	Email: <Your Email>

Assessment Overview

From <**Date**> through <**Date**>, 2020, <**Client**> engaged <**Your Name**> to evaluate the security posture of its infrastructure compared to current industry best practices that included a penetration test of the **Engagement Here**.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. **<Your Name>** will attempt to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. **<Your Name>** will

seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Scope

Assessment	Details
<Assessment Name>	Insert Information pertaining to the target scope

Scope Exclusions

The following shall be excluded from testing:
- Insert Exclusions Here

Client Allowances

The following is permitted by the client:
- Insert Allowances here

Executive Summary

<Your Name> evaluated <Client and Engagement Name>'s security posture through a penetration test from <Date> through <Date>, 2020. By leveraging a series of attacks, <Your Name> found vulnerabilities that allowed system or user level access to machines. It is highly recommended that <Client Name> address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Testing Summary

Insert Information pertaining to your testing summary here

The following table describes how <Your Name> gained partial or full control of each machine in <Client>'s testing subnet.

Step	Action	Recommendation
1	Insert Action you took to exploit the vulnerability – Example – Found default credentials on a Jenkins server	▪ Explain recommendations to remediate the situation ▪ Example – refer to organizational security policies and industry best standards to ensure proper password strength
2	Insert action you took to exploit the vulnerability	▪ See above
3	See above	▪ See above

Security Strengths

Insert a Strength Here

Explain the Strength

Insert a Strength Here

Explain the strength

Security Weaknesses

Insert a Weakness Here

Explain the weakness

Insert a Weakness here

Explain the Weakness

Penetration Test Findings

Insert the Vulnerability Here – Insert IP address or other information

Description:	Brief Description of the Vulnerability
Tools Used:	List the tools you used

Exploitation Proof of Concept

Explain your exploitation method here in about a paragraph. Include after this images and step by step instructions on how you exploited the service/machine.

<Insert Screenshots and Step by Step Instructions here>

Remediation

Who:	Describe Suggested Responsible Party (System Admin, Network Admin, etc)
Vector:	Remote or Local?
Action:	Item 1: Briefly explain the vulnerability again ▪ See above images for proof of exploit and associated instructions to reproduce Remediation: ▪ Reuse the remediation steps you described in the executive summary

Insert the Vulnerability Here – Insert IP address or other information

Description:	Brief Description of the Vulnerability
Tools Used:	List the tools you used

Exploitation Proof of Concept

Explain your exploitation method here in about a paragraph. Include after this images and step by step instructions on how you exploited the service/machine.

<Insert Screenshots and Step by Step Instructions here>

Remediation

Who:	Describe Suggested Responsible Party (System Admin, Network Admin, etc)
Vector:	Remote or Local?
Action:	Item 1: Briefly explain the vulnerability again ▪ See above images for proof of exploit and associated instructions to reproduce Remediation: ▪ Reuse the remediation steps you described in the executive summary

Copy and paste these for each machine you have to exploit

Last Page